IN THE CLAIMS:

1-50. (cancelled)

51. (currently amended) A method for printing of sensitive data, comprising the steps of:

at a workstation encrypting the sensitive data to be printed;

transferring the encrypted sensitive data to be printed along with non-sensitive data to be printed to a printing device having a printing unit;

decrypting the sensitive data to be printed to create decrypted sensitive data and in ~~an~~ immediate temporal succession converting the decrypted sensitive data to be printed into control signals for activation of the printing unit via rastering of the data into one or more raster images representing the control signals;

storing the decrypted sensitive data in a non-volatile memory such that the decrypted sensitive data are distributed in a plurality of memory segments of the non-volatile memory, and storing a relationship of the memory segments in said non-volatile memory in a volatile memory as relationship data independently of the stored decrypted sensitive data so that without said relationship data, the decrypted sensitive data stored in said memory segments is not readable; and

printing the non-sensitive data, and also printing the decrypted sensitive data based on the relationship data, with the printing unit on a recording medium.

52. (previously presented) The method according to claim 51 wherein the decryption and the conversion into control signals is executed in a controller for activation of a character generator.

53. (previously presented) The method according to claim 51 wherein the print data to be printed are transferred to the printing device in the form of a print

data stream, the print data stream being converted into an intermediate language in the printing device, and the print data being converted into the control signals.

54. (previously presented) The method according to claim 51 wherein the sensitive data and the non-sensitive data are connected into one data unit before transfer to the printing device.

55. (previously presented) The method according to claim 51 wherein the sensitive data are identified in the data unit via markings.

56. (previously presented) The method according to claim 54 wherein a layout that comprises regions to receive sensitive data is generated using the non-sensitive data.

57. (previously presented) The method according to claim 54 wherein the sensitive data are already encrypted before combination with the non-sensitive data into said one data unit.

58. (previously presented) The method according to claim 51 wherein the sensitive data are encrypted after combination with the non-sensitive data into said one data unit.

59. (previously presented) A system for printing sensitive data which have been encrypted, comprising:

a printing device having a printing unit connected to a controller, said controller receiving said encrypted sensitive data along with non-sensitive data;

said controller comprising a decryption module, a non-volatile memory, a relationship data volatile memory, and a converter which converts decrypted sensitive data from said decryption module in immediate temporal succession into control signals for activation of said printing unit, said control signals activating the

printing unit via rastering of the data into one or more raster images reprinting the control signals; and

said controller storing the decrypted sensitive data in said non-volatile memory such that the decrypted sensitive data are distributed in a plurality of memory segments of the non-volatile memory, and storing a relationship of the memory segments in said non-volatile memory in said relationship data volatile memory as relationship data independently of the stored decrypted sensitive data so that without said relationship data, the decrypted sensitive data stored in said memory segments is not readable.

60. (previously presented) The system according to claim 59 wherein the printing unit comprises a character generator.

61. (previously presented) The system according to claim 59 wherein the controller comprises at least one raster module as said converter.

62. (previously presented) The system according to claim 59 wherein the controller comprises a combined decryption and raster module.

63. (previously presented) The system according to claim 59 wherein a sensor for detection of recording media with predetermined security features is arranged on a transport path for recording media in a region before the printing unit such that the printing of the sensitive data can be stopped given detection of recording media without security features.